

**Cybersecurity for
Local Governments and Schools**

A Weekly Cybersecurity Awareness Month Web Series



NYS COMPTROLLER
THOMAS P. DiNAPOLI

Week 1 – IT Governance

Jessica Prevost-Allen, Municipal Auditor
Division of Local Government and School Accountability



NYS COMPTROLLER
THOMAS P. DiNAPOLI

Agenda
Top 12 Areas of Concern

1. IT Policy	7. Access Controls
2. IT Security Training and Awareness	8. Online Banking
3. Computer Hardware, Software and Data Inventories	9. Wireless Network
4. Contracts for IT Services	10. Firewalls and Intrusion Detection
5. Virus Protection	11. Physical Controls
6. Patch Management	12. IT Contingency Planning



NYS COMPTROLLER
THOMAS P. DiNAPOLI

Area #1: IT Policy

- Define appropriate user behavior, describe the tools and procedures needed to protect data and information systems, and explain the consequences of policy violations.
- Lack of policies and procedures increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access or use.



Area #1: IT Policy

- Required Policies:
 - Breach Notification
 - Section 208 (8) of the State Technology Law requires municipalities and other local agencies to have a breach notification policy or local law.
 - Data Security and Privacy
 - Section 2-d Part 121.5(b) of the State Education Law requires each educational agency to adopt and publish a data security and privacy policy.



Area #1: IT Policy

- Recommended Policies:
 - Online Banking
 - Acceptable Use
 - Other key topics to cover in policies
 - Password Security
 - Mobile Devices
 - Wireless Security



Area #2: IT Security Training and Awareness

- While the IT policies tell computer users what to do, cybersecurity training provides them with the skills to do it.
 - IT security awareness training should explain the proper rules of behavior for using your IT systems and data, as well as communicate the policies and procedures that need to be followed.
- Failure to provide IT security awareness training increases the risk that users will not understand their responsibilities, putting the data and computer resources at risk for unauthorized access, misuse or abuse.

Area #2: IT Security Training and Awareness

- State Education Law (§2-d) and the Regulations of the Commissioner of Education (Part 121.7) require educational agencies to annually provide data privacy and security awareness training to their officers and employees with access to personally identifiable information. The training must cover the federal and State laws governing the confidentiality of personally identifiable information of students, teachers and principals, and how employees can comply with those laws.

Area #2: IT Security Training and Awareness

Possible Training Topics to Consider:

- | | |
|---|--------------------------------------|
| • Disaster Recovery Procedures | • Acceptable Use Policy Requirements |
| • Physical Security, Clean Desk, Environmental Controls | • Social Networking Dangers |
| • Mobile/Removable Devices | • Malware |
| • Bring-Your-Own-Device (BYOD) | • Email Scams (phishing) |
| • Data Classification (PPSI) | |
- Training does not have to be elaborate or expensive!**

Area #2: IT Security Training and Awareness

Organizations offering free or low-cost IT security training and awareness materials:

- Center for Internet Security
 - <https://www.cisecurity.org/>
- New York State Office of Information Technology Services
 - <https://its.ny.gov/>
- New York State Office of the State Comptroller
 - <https://www.osc.state.ny.us/>
- United States Cybersecurity and Infrastructure Security Agency
 - <https://www.cisa.gov/>
- New York State Education Department
 - <http://www.nysed.gov/data-privacy-security>

Municipal and school district associations (e.g., New York Conference of Mayors, New York State School Boards Association) also offer low-cost cybersecurity training.

Area #3: Computer Hardware, Software and Data Inventories

- Organizations should maintain detailed, up-to-date inventory records for all computer hardware, software and data.

Area #3: Computer Hardware, Software and Data Inventories

- Hardware information to maintain:
 - A description of the item including the make, model and serial number.
 - The name of the employee to whom the equipment is assigned.
 - The physical location of the asset.
 - Relevant purchase or lease information, including the acquisition date.

Area #3: Computer Hardware, Software and Data Inventories

- Software inventory records should include:
 - A description of the item, including the version and serial number.
 - A description of the computer(s) on which the software is installed.
 - Any pertinent licensing information.

Area #3: Computer Hardware, Software and Data Inventories

- Maintain an inventory of information assets that classifies the data according to its sensitivity and identifies where the data resides.

Area #3: Computer Hardware, Software and Data Inventories

- Data classification scheme example:
 - Public
 - Widely available to the public.
 - Internal use
 - Unauthorized access, modifications or disclosure would be inconvenient but would not result in financial loss or damage to public credibility.
 - Confidential
 - Unauthorized access, modifications or disclosure could result in significant adverse impacts on an organization's ability to perform critical work or compromise the integrity of the organization, its employees, its customers or third parties.
 - Restricted Confidential
 - Loss, unauthorized modifications or disclosure is likely to result in the most serious impacts to an organization's ability to fulfill its responsibilities.

Area #4: Contracts for IT Services

- Establish specific measurable performance targets
 - Examples:
 - Patch management is provided daily, weekly or as updates are released.
 - Cloud service provider guarantees access to application a percentage of time and reduces fee if unable to meet target.
- Needed due to increasing reliance on third-party IT-related services
- Provides protection and helps avoid misunderstandings
 - Responsibilities of vendor are clearly defined so IT operations function as intended and IT assets are protected.

Area #4: Contracts for IT Services

- State Education Law requirements in any contract that involves sharing of personally identifiable information of students, teachers or principals with the third-party contractor.

Area #5: Virus Protection

- Detect and stop some forms of malware
- Should be installed and kept current with software and signature updates
 - Update definitions daily
 - Scan for threats throughout the day

Area #6: Patch Management

- Patches update software programs with important information that could potentially protect systems running those programs from attacks.
 - Outdated or unsupported software leaves organizations vulnerable.

Area #7: Access Controls

- Computer access controls prescribe who or what computer process may have access to a specific computer resource, such as a particular software program or database.
 - Limited access reduces risk that outsiders can gain unauthorized access to systems or data.
 - Access to sensitive resources should be limited based on job duties.
 - Written procedures for granting, changing and revoking access to the network, individual computer systems and specific software applications should be in place.

Area #7: Access Controls

Password Recommendations

- Length
 - Should be at least eight characters.
 - As the number of characters in a password increases, the strength of the password increases exponentially.
 - 8-character password has 78 million times the possible combinations than that of a 4-character password; in terms of time, that is one second versus 903 days.
- Complexity Requirements
 - At least one uppercase character, one lowercase character, one numeric character and one special character (e.g., %, #, @).
 - Not include names or words that can be easily guessed or identified using a password-cracking mechanism or dictionary.
 - Should not contain any part of the account, network or municipality names.

Area #7: Access Controls

Password Recommendations

- Aging
 - Changed at least every 60 days.
- Failed Log-On Attempts
 - Limited to 10 or fewer consecutive failed attempts.
 - Automatic lockout for a duration of at least 15 minutes or until an administrator manually unlocks.

Area #8: Online Banking

- Fraud involving the exploitation of valid online banking credentials is a significant risk facing any local government or school district that processes financial transactions online.
- Organizations should have a combination of nontechnical and technology-based controls in place to safeguard against online banking fraud.
- A further discussion of online banking controls can be found in the State Comptroller's publication entitled *Local Government Management Guide: Cash Management Technology*.

Area #9: Wireless Network

- Wireless networks are exposed to many of the same types of threats and vulnerabilities as wired networks, including viruses, malware, unauthorized access and data loss.

Area #9: Wireless Network

Best Practices

- Adopting written policies and procedures.
- Determining the optimal number, physical location and broadcasting power of wireless access points.
- Maintaining an inventory of and monitoring wireless access points
- Changing the service set identifier (the SSID or name of the wireless network) using a naming convention that excludes identifiable information about the organization, location, technology, manufacturer and type of data traversing the network.
- Requiring an access password for users and enabling the most secure encryption available (currently WPA2 or WPA3).
- Changing the administrative password (used by the administrator to set up the wireless access point) from its well-known default value.
- Updating and patching all software and hardware devices in a timely manner.
- Considering other security controls that may be necessary given the organization's unique computing environment and security needs.

Area #10: Firewalls and Intrusion Detection

- Firewalls
 - Hardware and/or software programs that enforce boundaries between devices on different networks or network segments.
 - Should configure firewall rules to allow only those communication types that are needed for system operations and explicitly deny all other communications.
 - Effective tracking tools.

Area #10: Firewalls and Intrusion Detection

- Intrusion Detection
 - Monitor the events occurring in a computer system or network and analyze them for signs of possible incidents.
 - Network-based intrusion detection systems (IDS) capture and analyze network communications within a network or network segment.
 - Host-based IDSs capture and analyze activity to and from a particular computer.

Area #10: Firewalls and Intrusion Detection

- IDS should be implemented to selectively identify unauthorized, unusual and sensitive access activity, such as:
 - Attempted unauthorized access.
 - Deviations from access trends.
 - Access to sensitive data and resources.
 - Highly sensitive privileged access, such as the ability to override security controls.
 - Floods of data coming from or going to a particular system or group of systems.
 - Access modifications made by security personnel.
 - Multiple consecutive unsuccessful attempts to log on to a system.

Area #11: Physical Controls

- Physical security controls restrict physical access to computer resources and protect these resources from intentional or unintentional harm, loss or impairment.
 - Guards, gates and locks
 - Environmental controls
 - Smoke detectors, fire alarms and extinguishers, protection from water damage, and uninterruptible power supplies.

Area #12: IT Contingency Planning

- The plans, policies, procedures and technical measures that enable the recovery of operations after an unexpected IT disruption.
- The goal is to enable a computer system and/or electronic data to be recovered as quickly and effectively as possible following an unplanned disruption.

Area #12: IT Contingency Planning

Best Practices

- Assemble a team responsible for drafting the plan.
- Identify and prioritize critical business processes and services.
- Develop and distribute the plan to all responsible parties.
- Train personnel expected to execute the plan.
- Test the plan.
- Review and revise the plan.

Area #12: IT Contingency Planning

Backup Procedures

- A backup is a copy of data files and software programs made to replace original versions if there is loss or damage to the original.
- Procedural Best Practices
 - Adopt a backup policy that defines frequency, scope, storage location(s) and specific method(s) for backups.
 - Back up data at intervals appropriate for the organization's data needs and usage.
 - Verify data has been backed up and can be restored whenever needed.
 - Store backups in an offline and offsite location.

Security Self-Assessment

- Addresses key areas of IT internal controls such as policy, training, access and monitoring.
- Several of the main questions include follow-up questions that will provide information helpful for evaluating the answers.

Resources

Office of the State Comptroller, IT Governance

<https://www.osc.state.ny.us/files/local-government/publications/pdf/itgovernance.pdf>

Multi-State Information Sharing & Analysis Center (MS-ISAC)

<https://www.cisecurity.org/blog/a-new-vision-for-cyber-threat-intelligence-at-the-ms-isac/>

<https://nist.gov>

New York State Office of Information Technology Services (NYS ITS)

<https://its.ny.gov>

Cybersecurity and Infrastructure Security Agency (CISA)

<https://www.cisa.gov>



34

Sneak Peek - Week 2

IT Contingency Planning

- What is IT Contingency Planning?
- IT Contingency Planning Best Practices
- Backup Procedures
- Backup Procedure Preventive Controls
- Backup Procedure Best Practices



35

Thank You



Division of Local Government and School Accountability
LGSAAppliedTech@osc.ny.gov



36
